

January 23, 2024

Challenge yourself with our Quishing Quiz!

Cybersecurity Issue of the Week: **Malware**

🌐 There's different types of malware. Check out our **Spyware Infosheet** to learn more.

Wonder what you can do to protect yourself from malware?

All Users	Technical Users	Business Owners
Never click on suspicious looking advertising links on websites, especially websites you're not familiar with or look suspicious themselves.	In general, try to avoid clicking on any advertising links on sites that you are unfamiliar with.	Periodically create system backups in case a malware attack succeeds.

This past week's stories:

🍁 **Are passwords of the past? N.B. cyber expert on emerging debate over passkeys**

🍁 **City moves to upgrade cybersecurity as new details emerge about ransoms in recent attacks**

🍁 **Think boomers are most vulnerable to cybersecurity attacks? Wrong. It's actually Gen Z**

What is credential stuffing and how can I protect myself? A cybersecurity researcher explains

AI, gaming, fintech named major cybersecurity threats for kids

Cyber attacks on Kent councils disrupt online services

Hackers abuse TeamViewer to launch ransomware attacks

2024 cybersecurity predictions: The continued rise of AI and regulation

🌐 **Pure malware tools masquerade as legitimate software to bypass detections**

Court charges dev with hacking after cybersecurity issue disclosure

North Korean hackers weaponize fake research to deliver RokRAT backdoor

New Bluetooth vulnerability let hackers takeover of iOS, Android, Linux, & MacOS devices

Are passwords of the past? N.B. cyber expert on emerging debate over passkeys

It may be a foreign concept to some but for others, it's a natural technological progression: Passkeys.

<https://www.cbc.ca/news/canada/new-brunswick/passwords-passkeys-cybersecurity-1.7088680>

Click above link to read more.

[Back to top](#)

City moves to upgrade cybersecurity as new details emerge about ransoms in recent attacks

In the wake of cyberattacks on the public library and zoo, Toronto is moving to consolidate security for all its agencies, belatedly heeding warnings that the city's scattered system is vulnerable.

https://www.thestar.com/news/gta/city-moves-to-upgrade-cybersecurity-as-new-details-emerge-about-ransoms-in-recent-attacks/article_f8172350-b62b-11ee-b06e-dfb077b08510.html

Click above link to read more.

[Back to top](#)

Think boomers are most vulnerable to cybersecurity attacks? Wrong. It's actually Gen Z

For many Gen Z-ers, posting "get to know me" videos on social media is a fun way to connect with their followers.

<https://www.cbc.ca/news/canada/calgary/gen-z-cybersecurity-1.7088579>

Click above link to read more.

[Back to top](#)

What is credential stuffing and how can I protect myself? A cybersecurity researcher explains

Cyber-skullduggery is becoming the bane of modern life. Australia's prime minister has called it a "scourge", and he is correct. In 2022–23, nearly 94,000 cyber crimes were reported in Australia, up 23% on the previous year.

<https://techxpire.com/news/2024-01-credential-stuffing-cybersecurity.html>

Click above link to read more.

[Back to top](#)

AI, gaming, fintech named major cybersecurity threats for kids

The heightened utilization of AI tools and potential vulnerabilities in gaming have been identified as crucial cybersecurity concerns for children in 2024, according to a new report by Kaspersky.

<https://www.infosecurity-magazine.com/news/ai-gaming-fintech-kids/>

Click above link to read more.

[Back to top](#)

Cyber attacks on Kent councils disrupt online services

Cyber attacks have disrupted online services for three councils in Kent.

Canterbury City Council and Dover District Council said they were investigating "incidents".

<https://www.bbc.com/news/uk-england-kent-68023647>

Click above link to read more.

[Back to top](#)

Hackers abuse TeamViewer to launch ransomware attacks

Hackers exploit TeamViewer because it gives remote access to systems and allows threat actors to control them.

<https://cybersecuritynews.com/hackers-abuse-teamviewer/>

Click above link to read more.

[Back to top](#)

2024 cybersecurity predictions: The continued rise of AI and regulation

The last 12 months have been seismic for cybersecurity, with successful hacks and breaches continuing to make front-page news. The task of keeping networks and data safe is an ever-evolving one, with hackers and cybersecurity professionals in a constant state of cat-and-mouse as they try to outsmart one another.

<https://betanews.com/2024/01/18/2024-cybersecurity-predictions-the-continued-rise-of-ai-and-regulation/>

Click above link to read more.

[Back to top](#)

Pure malware tools masquerade as legitimate software to bypass detections

Recently, security analysts at ANY.RUN discovered that the Pure malware tools are masquerading as legitimate software to evade detection.

<https://cybersecuritynews.com/pure-malware-tools/>

Click above link to read more.

[Back to top](#)

Court charges dev with hacking after cybersecurity issue disclosure

A German court has charged a programmer investigating an IT problem with hacking and fined them €3,000 (\$3,265) for what it deemed was unauthorized access to external computer systems and spying on data.

<https://www.bleepingcomputer.com/news/security/court-charges-dev-with-hacking-after-cybersecurity-issue-disclosure/>

Click above link to read more.

[Back to top](#)

North Korean hackers weaponize fake research to deliver RokRAT backdoor

Media organizations and high-profile experts in North Korean affairs have been at the receiving end of a new campaign orchestrated by a threat actor known as ScarCruft in December 2023.

<https://thehackernews.com/2024/01/north-korean-hackers-weaponize-fake.html>

Click above link to read more.

[Back to top](#)

New Bluetooth vulnerability let hackers takeover of iOS, Android, Linux, & MacOS devices

Bluetooth vulnerabilities in Android, Linux, macOS, iOS, and Windows are critical as hackers could exploit them to gain unauthorized access to the vulnerable devices.

<https://cybersecuritynews.com/bluetooth-flaw-hackers-takeover/>

Click above link to read more.

[Back to top](#)

Click [unsubscribe](#) to stop receiving the Digest.

The Security News Digest (SND) is a collection of articles published by others that have been compiled by the Information Security Branch (ISB) from various sources. The intention of the SND is simply to make its recipients aware of recent articles pertaining to information security in order to increase their knowledge of information security issues. The views and opinions displayed in these articles are strictly those of the articles' writers and editors and are not intended to reflect the views or opinions of the ISB. Readers are expected to conduct their own assessment on the validity and objectivity of each article and to apply their own judgment when using or referring to this information. The ISB is not responsible for the manner in which the information presented is used or interpreted by its recipients.

For previous issues of Security News Digest, visit the current month archive page at:

<http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/security-news-digest>

To learn more about information security issues and best practices, visit us at:

<https://www.gov.bc.ca/informationsecurity>

OCIOSecurity@gov.bc.ca

The information presented or referred to in SND is owned by third parties and protected by copyright law, as well as any terms of use associated with the sites on which the information is provided. The recipient is responsible for making itself aware of and abiding by all applicable laws, policies and agreements associated with this information.

We attempt to provide accurate Internet links to the information sources referenced. We are not responsible for broken or inaccurate Internet links to sites owned or operated by third parties, nor for the content, accuracy, performance or availability of any such third-party sites or any information contained on them.



Security News Digest

Information Security Branch



OCIO

Office of the
Chief Information Officer